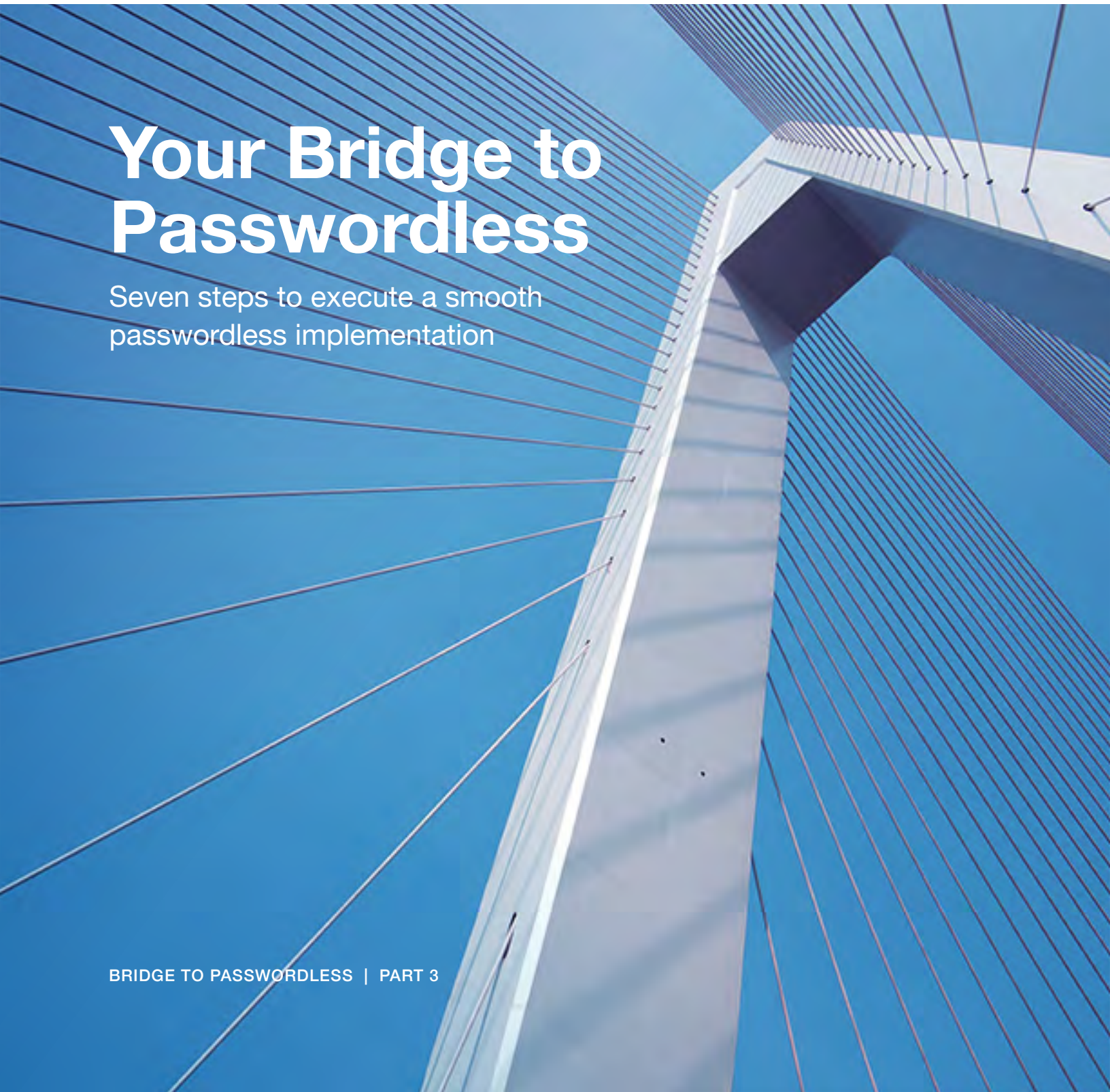
yubico



Your Bridge to Passwordless

Seven steps to execute a smooth passwordless implementation

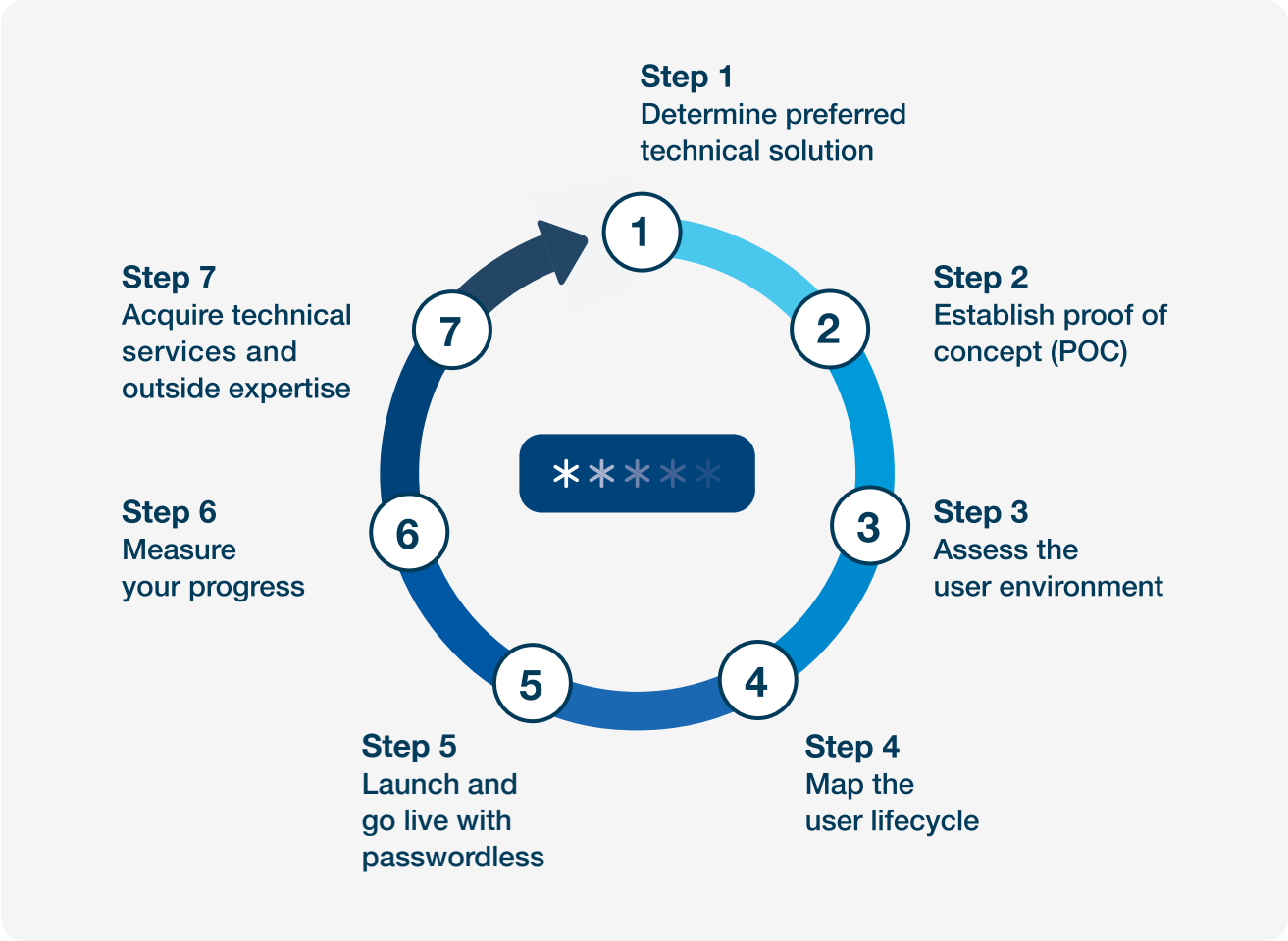
BRIDGE TO PASSWORDLESS | PART 3

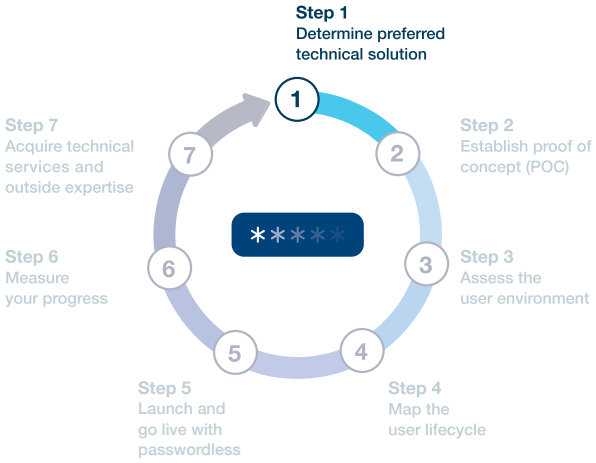
Ready to start passwordless?

We've talked about many of the early considerations when traveling the road to a passwordless future, given how fast you want to progress and which users to bring along first on that journey. At some point the enterprise will decide it's time to take the next step (or several) toward passwordless, whether that involves a smart card passwordless approach, a FIDO2/WebAuthn passwordless approach, or a hybrid approach of combining multiple approaches for different business needs. This paper will outline concrete steps to take when you are ready to plan and execute deployment of your passwordless solution. Keep in mind that these steps aren't all perfectly chronological, so some initiatives may overlap on the timeline or run in parallel.

Seven steps in a successful passwordless deployment project

Approaching the implementation with a best practices and methodical approach that is inclusive of key stakeholders in the organization leads to the desired outcome of greater security with enhanced productivity.



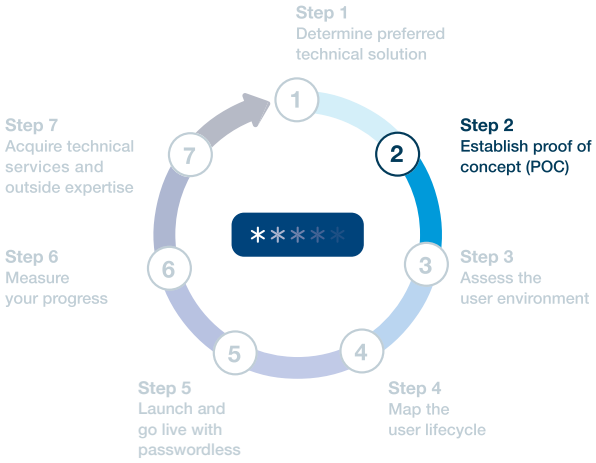


Step 1
Determine preferred technical solution

When you're at the starting line, there are a few early steps you can take to make sure your organization is prepared. Begin by assessing your existing technical environment. While every solution approach may vary, below are a few basic rules of thumb that will point you in the right direction:

- If you have already transitioned to a cloud-first environment then you'll be able to easily implement FIDO2 passwordless. Typically a cloud-first environment will operate in Azure AD (or a hybrid of AAD and AD) and use applications like Office365 or other SaaS applications federated with AAD. There may also be a different Identity Provider (IdP) system in place.

- If you are operating in an on-premises Active Directory (AD) environment, then a smart card passwordless implementation is probably your best choice. These environments will not be conducive to pursuing a FIDO2/WebAuthn passwordless strategy, as today the ecosystem is mainly geared towards cloud-first scenarios.
  - Note: In a hybrid AAD/AD environment, it's possible to implement both a smart card implementation (for elevated admin-level users) and FIDO2 (for all other users).
- If you have an existing IAM provider, you will need to determine whether they are mostly on-premises or cloud-led. Complexity may determine whether you can fully implement a FIDO2/WebAuthn solution or opt for a more incremental approach.



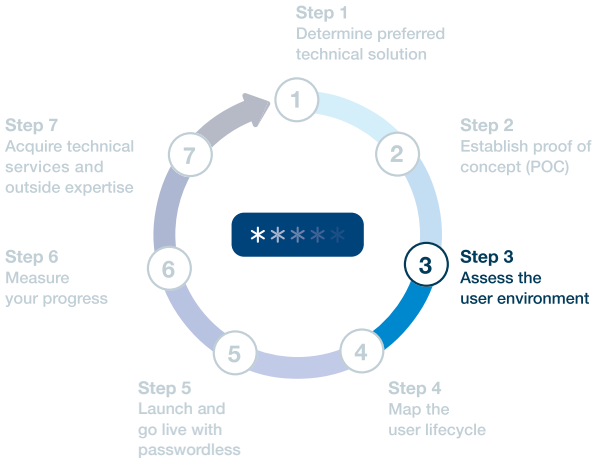
Step 2
Establish proof of concept (POC)

Technical validation via a “proof of concept” (POC) for your passwordless strategy is a solid next step. Typically a POC is a precursor to a pilot with a small user group, followed by a full-scale launch/go-live.

Below are some items to help you get started:

- Validate the intended passwordless implementation works as expected with the essential systems, use cases, and users at the earliest phase.
- Set up a testing environment that demonstrates end-to-end connectivity between existing systems and authentication technology, for key users/user groups.
- Validate that your defined success criteria can be met.

Step 3
Assess the user environment



The next step is to look closely at the user environment and gain a detailed understanding of needs, behaviors, devices used and access points. By the end of this assessment you should have a solid understanding of:

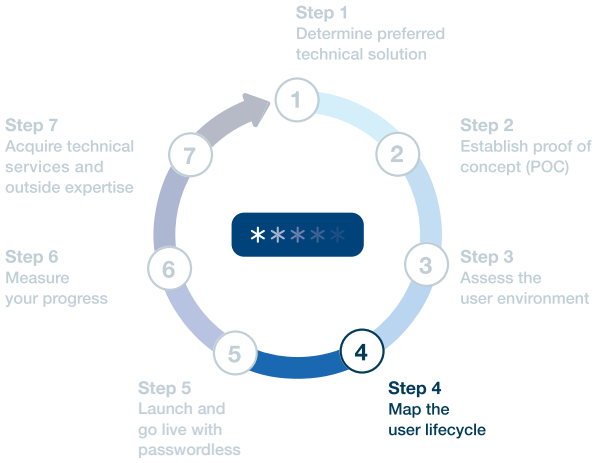
Users and use cases
Consider every user's needs, current behavior, risk profiles and experience metrics. Log the type of devices users are utilizing so you can design a better passwordless experience with these in mind. Do most of your users access the system through mobile devices, workstations or both? Do they share workstations? Depending on that device inventory, some full FIDO2/WebAuthn passwordless solutions may be limited. If an organization operates in a bring-your-own-device (BYOD) or mixed device environment, a smart card passwordless or hybrid implementation may be a better option.

Cross-functional alignment
Identifying all stakeholders as well as meeting with and reviewing your plans will ensure all parties are on the same page and participating in the journey. It is beneficial to the overall process if all stakeholders have a common understanding of what passwordless is, how it will help enhance organizational security, improve the user experience and deliver cost benefits through reduced calls to the helpdesk, and less employee downtime. Ultimately, adding new or enhancing existing authentication flows into the environment often touches many parts of the organization, not just IT functions, so buy-in and collaboration is important.

Workforce location
The location of your users and how you will provide them access to the technology is good to consider. If you are considering mobile authentication, then you can leverage devices your users already have. However, it is worth noting that there are some security risks with this approach. On the other hand, if you are considering hardware-based security keys for users which offer the strongest form of protection, the location of your workforce and distribution must be part of the strategic plan. If a significant portion of your workforce will be working remotely, you will want to find an efficient way to distribute, activate and re-credential users through a self-service provisioning process. There are some turnkey delivery solutions available, where all the delivery logistics to users at corporate and residential locations are managed by the authentication provider. This may be an option as well as bringing distribution in-house if the resources are available.

Step 4
Map the user lifecycle

If the modern MFA approach to deliver secure passwordless involves hardware security keys, then the next steps in the journey are critical. Apart from technology decisions and planning, operational readiness must also be taken into account. Below are a few elements of the user lifecycle to consider prior to launching a passwordless solution.



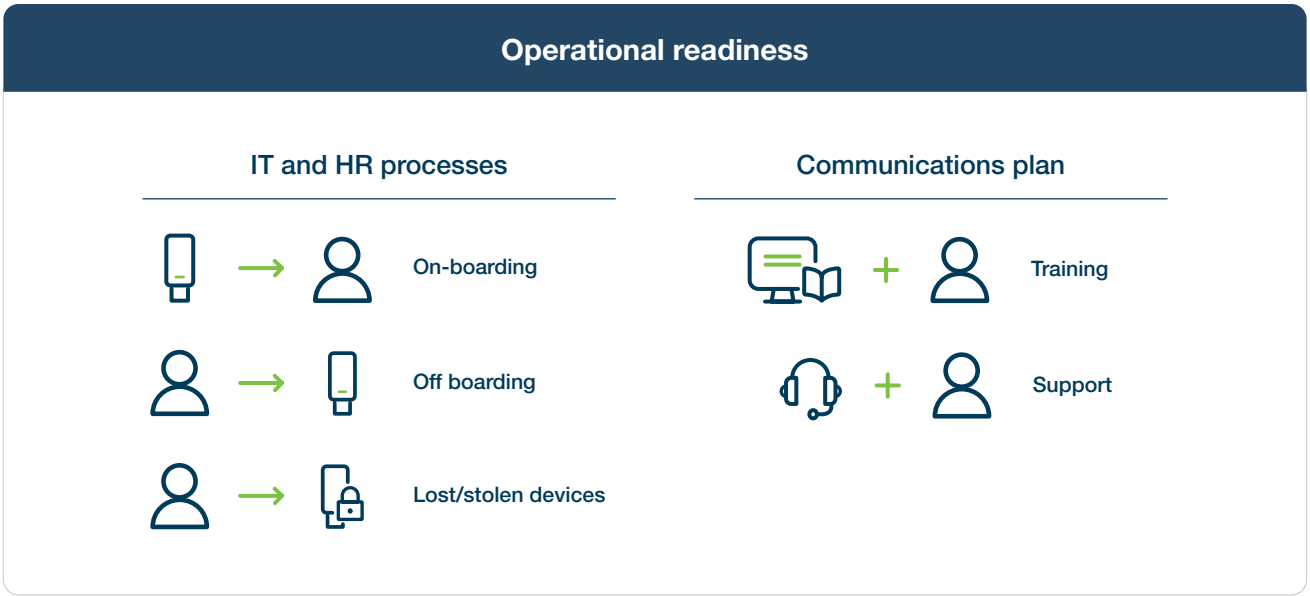
Technical HR processes

Define a clear plan for how a security key fits into existing HR processes:

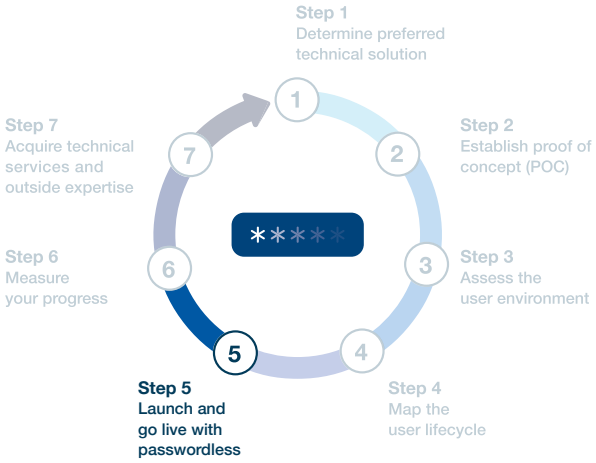
- On-boarding - how security are keys provided to new employees including how users then activate keys.
- Off boarding - how are credentials revoked for exiting employees or how are employees who may be on extended leave managed.
- Lost/stolen devices - how are lost or stolen keys deactivated and how do users obtain and activate replacement keys.

Training and support

A communications and training plan is essential for smooth adoption of authentication technologies. A communication plan should be developed with IT, HR and any other communications experts within the organization. Assets and resources should be readily available to those who are on-boarding new users and supporting existing ones. A higher level of support for users may be necessary to make sure productivity isn't compromised as they learn new security best practices. Training and support will be essential to have a successful deployment.



Step 5
Launch and go live with passwordless



As you step through all of the industry best practices when planning a passwordless implementation, you will arrive at the point where it's important to see if all aspects are ready, and how it all works in tandem:

Always launch a pilot before full go-live:

- You can plan for a single pilot, or you may want to deploy several pilots targeting different user groups to measure readiness before a broader rollout to all users.

An exception if timeline is short:

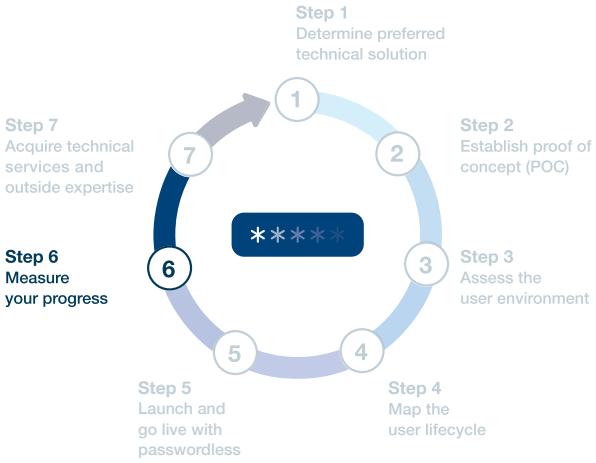
- Sometimes there's more urgency than you'd like (for example, after a breach when you are trying to patch a vulnerability) and you don't have time for a full pilot. In those cases you can consider skipping a pilot and relying on your "proof of concept" data you acquired earlier to stand in as a substitute. This is generally considered only in situations where a comprehensive pilot must be traded for urgency of action.

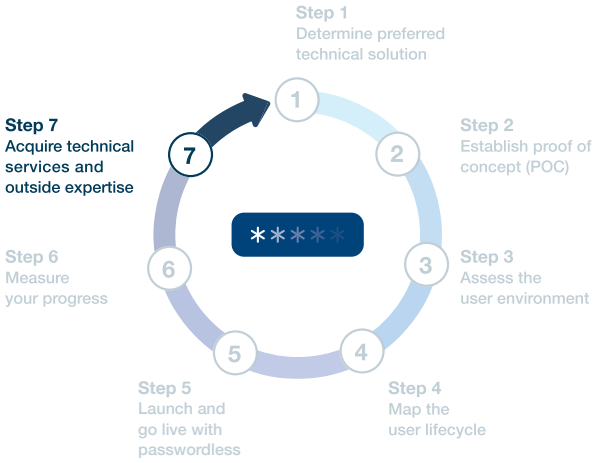
- The communications/training team can help in this area by planning live or virtual events that build anticipation and greater understanding of the new solutions and processes. If users are celebrating the launch (and are incentivized to learn more about it), they are likely to adopt it more quickly.
- Create launch activities that build buzz and excitement. You want your users to understand how this will help simplify their daily activities, to be excited about the change, and why this is important to the organization, rather than viewing it as another process they're being burdened with.

Step 6
Measure your progress

The right metrics will help you demonstrate success and monitor the progress of your passwordless deployment. They might include:

- If you are using hardware-based keys, how many have been shipped/received.
- Performance metrics, such as the percentage of authentications leveraging the passwordless solution in your organization.
- Impact on help desks such as call volume and the reduced number of password-related tickets.
- Overall financial benefits/assessment. For example, help desk cost per call savings or reduced user downtime.





Step 7
Acquire technical services and outside expertise

The road to passwordless can take time and include a variety of considerations to minimize surprises or unexpected twists. It's worth doing an honest assessment of your organization's internal resources to determine what technical resources you have available to launch a passwordless solution. Leveraging experts who have successfully traveled this road before will help fast track progress and overall success.

A few things to consider:

- What's your timeline? If you are on a tight deadline, industry expertise from an outside source might help accelerate the passwordless journey.
- Where can professional services (PS) help? For most organizations this will be the first dip into the passwordless waters, so it helps to have an experienced party extend or support your team. PS consultants can help build a roadmap, design workshops and training programs, build on best practices, and help assemble a fully supported integration plan.
- PS can be especially helpful if you have multiple use cases or complex security environments/architecture (for example, working with an Azure AD environment, a smart card system and a Cisco VPN all at the same time).

YubiKey 5 Series as the bridge toward passwordless

Once you recognize that passwordless will be a journey it will be clear that flexible tools will be needed to help you reach your final destination. Consider a security solution that addresses your needs as your business evolves. The YubiKey 5 Series is a multi-protocol, passwordless security solution compatible across a full range of environments, from legacy to modern environments, across desktop and mobile. The YubiKey 5 Series can enable you to leverage the investments in your environment that you have already made. In this respect, YubiKeys will act as your bridge to passwordless—supporting you every step of the way, and future-proofing your security investment as your needs continue to evolve.

You can learn more about how to accelerate your passwordless deployment with Yubico's professional services here.

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.